CSC-EPL-89/007

2

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF MICRONYX INCORPORATED

TRISPAN

30 September 1989

Approved for Public Release:
Distribution Unlimited

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

3. DISTRIBUTION/AVAILABILITY OF REPORT
UNLIMITED DISTRIBUTION

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
CSC-EPL--SUM-89/007

5. MONITORING ORGANIZATION REPORT NUMBER(S)
S234,966

6a. NAME OF PERFORMING ORGANIZATION
National Computer Security Center

6b. OFFICE SYMBOL (If applicable) C12

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS (City, State and ZIP Code)

9800 Savage Road
Ft. George G. Meade, MD 20755-6000

7b. ADDRESS (City, State and ZIP Code)

8a. NAME OF FUNDING/SPONSORING ORGANIZATION

8b. OFFICE SYMBOL (If applicable)

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS (City, State and ZIP Code)

10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.

11. TITLE (Include Security Classification)
Final Evaluation Report Micronyx Incorporated TRISPAN

12. PERSONAL AUTHOR(S)
Deborah M. Clawson; Michael J. Oehler; Shawn M. Rovansek

13a. TYPE OF REPORT
Final

13b. TIME COVERED
FROM ____ TO ___

14. DATE OF REPORT (Yr, Mo., Day)
890930

15. PAGE COUNT
40

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB. GR.

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
NCSC, I&A, DAC, AUD, Micronyx, TRISPAN, CSSI

19. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Micronyx Incorporated TRISPAN has been evaluated by the National Computer Security Center (NCSC). The security features of the TRISPAN were examined against the requirements specified by the *COMPUTER SECURITY SUBSYSTEM INTERPRETATION OF THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (CSSI) dated 16 September 1988.* The NCSC evaluation team has determined that the TRISPAN has some I&A/D2 class features, however, all requirements of a given class must be met for a subsystem to receive that rating. It has been determined that the highest class at which the TRISPAN satisfies all the specified requirements of the CSSI is class I&A/D., DAC/D, and Audit/D

This report documents the findings of the evaluation.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
UNCLASSIFIED/UNLIMITED

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
DENNIS E. SIRBAUGH

22b. TELEPHONE NUMBER (Include Area Code) (301)859-4458

8b. OFFICE SYMBOL
C12

EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

91 4 25 027

FINAL EVALUATION REPORT

MICRONYX INCORPORATED

TRISPAN

NATIONAL
COMPUTER SECURITY CENTER

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

30 September 1989

This page intentionally left blank.

FOREWORD

This publication, the Final Evaluation Report of Micronyx's TriSpan, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center". The purpose of this report is to document the results of the TriSpan evaluation. The requirements stated in this report are taken from the *COMPUTER SECURITY SUBSYSTEM INTERPRETATION* of the *DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA* dated 16 September 1988.

Approved:

Thomas R. Malarkey,
Acting Chief,
Office of Product Evaluations
and Technical Guidelines
National Computer Security Center

30 September 1989

ACKNOWLEDGEMENTS

Team Members

Team members included the following individuals, who were provided by the following organizations:

Captain Deborah M. Clawson, USAF
Michael J. Oehler
Shawn M. Rovansek

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

CONTENTS

EXECUTIVE SUMMARY

The National Computer Security Center (NCSC) examined the security protection mechanisms provided by Micronyx's TriSpan Version 1.1230. TriSpan is a subsystem, not a complete trusted computer system. Therefore, it was evaluated against the *Computer Security Subsystem Interpretation* (CSSI). Specifically, the applicable requirements for this evaluation included identification & authentication (I&A), discretionary access control (DAC), and audit.

The evaluation team determined that the highest class at which TriSpan satisfies the I&A, DAC, and the audit requirements of the CSSI is class D. The final rating of D for each of the three evaluated features resulted from TriSpan's inability to meet all assurance and documentation requirements specified by the CSSI. See page 25, "Rating Assignment", for a description of each component in the rating.

To obtain the level of trust described in this report, TriSpan must be configured in accordance to the caveats of this report and the *Workstation Administrator's Guide* (WAG), included as part of TriSpan's documentation set. Additionally, administrators must be aware of the functions and capabilities of the programs residing on the system so that the greatest assurance can be achieved. Most notably, administrators must account for DOS's files, programming languages, compilers, utilities, and TriSpan's commands. Administrators may restrict access to these programs for certain users by using TriSpan's protection mechanisms.

Subsystems are designed to be installed on automatic data processing (ADP) systems. Specifically, subsystems are designed to add a level of assurance to an ADP system that has limited or ineffective security mechanisms. However, subsystems are not intended to protect information on an ADP system which processes classified information because subsystems may not be capable of maintaining the integrity of classified information.

This page intentionally left blank.

INTRODUCTION

In May 1989, the National Computer Security Center (NCSC) began a product evaluation of Micronyx Incorporated's TriSpan. The objective of this evaluation was to rate TriSpan against the *Computer Security Subsystem Interpretation* (CSSI), and to place it on the Evaluated Products List (EPL) with a final rating for each of TriSpan's components. This report documents the results of the evaluation. This evaluation applies to TriSpan Version 1.1230 available from Micronyx Incorporated.

Material for this report was gathered by the NCSC TriSpan evaluation team, through documentation, interaction with system developers, and through the use of TriSpan.

Evaluation Process Background

The National Computer Security Center (NCSC) was created to improve the state of computer security in computer systems processing information that is vital to the owners of that information. The Center fulfills its mission by promoting the development and implementation of Trust Technology and encouraging the widespread availability and use of trusted computer security products. Through the Trusted Product Evaluation Program, the Center works with the manufacturers of hardware and software products to implement and make available to the public good computer security solutions. Under this program, the NCSC evaluated the technical protection capabilities of computer security products against well-defined published evaluation criteria.

The product evaluation process culminates in the publication of a Final Evaluation Report, of which this document is an example. The Final Evaluation Report describes the product and assigns it a rating that denotes a specific level of trust. The assigned rating is independent of any consideration of overall system performance, potential applications, or particular processing environment. Rated products are listed on the Evaluated Products List (EPL), the aim of which is to provide ADP system developers, managers, and users an authoritative evaluation of a product's suitability for use in processing important information.

The NCSC Computer Security Subsystem Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the NCSC's Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations. Security Managers should note that subsystems are not capable of protecting information with sufficient assurance to maintain classified information on a system protected solely by security subsystems. Furthermore, subsystems may not be used to upgrade the protection offered by complete trusted systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added to other protection devices to provide another layer of security, but in no way may be used as justification for processing classified material.

Subsystems considered in the program are special purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment.

To promote consistency in evaluations, subsystems' security mechanisms are assessed against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC). Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, an evaluation report will assign a specific rating for each of the components of the subsystem and a summary of the evaluation report will be placed on the Evaluated Products List (EPL) which is maintained in the *Information Systems Security Products and Services Catalog.*

Document Organization

This report consists of four major sections and three appendices. Section 1 is an introduction. Section 2 provides an overview of the system's hardware and software architecture. Section 3 provides a mapping between the requirements specified in the CSSI, and the features and assurances that fulfill those requirements. Section 4 presents the evaluation team's comments of the subsystem. The appendices identify specific hardware and software components to which the evaluation applies, and also a glossary of terms.

For consistency with documentation presented by Micronyx, this report uses the term "workstation" to refer to the IBM PC, XT, and IBM AT. However, the report will refrain from using the terms "labels", "access level", and "Mandatory Access Control" as stated in Micronyx's documentation, because they differ from that in the TCSEC.

SYSTEM OVERVIEW

Background and History of Micronyx

Established in 1976, Micronyx is a privately held corporation dedicated to the development and manufacturing of engineering services. As part of those services, Micronyx has been involved in secure product development for microcomputers since 1985. Micronyx's family of workstation control products includes Triumph! and TriSpan. In addition to workstation control, Micronyx has developed an audit analysis tool, called Browser, and an integration support package which provides developers access to a C language library so that their applications can call TriSpan's capabilities.

Product Overview

TriSpan is one of a family of products from Micronyx used to manage and control access to a workstation running a single-tasking version of the MS-DOS operating system. The product consists of a hardware card, electronic key-ringed sized tokens, administrative and user documentation, and application software used to configuration its security features. Once installed, TriSpan provides a degree of I&A, DAC and audit functionality. TriSpan uses the electronic tokens to authenticate the identity of users and controls access to protected files based upon that identity. TriSpan's auditing can be configured and will record a variety of events. Overall, the operation is transparent and uses a normal DOS environment without imposing a custom command shell.

Although not a part of the evaluated configuration, TriSpan provides some additional functionality. These include file overwrites, restricted shell mode, a "SCRIPTER" mode to direct users to their directories and application programs, and LAN based protection and configuration of the product. These functions are beyond the scope of the CSSI or can not fully meet the requirements of the CSSI, but may still be of interest to some.

A complete description of TriSpan architecture, the resources it protects, and its security mechanisms relative to the CSSI follows.

Security Relevant Portion

The protection-critical mechanism or the Security Relevant Portion (SRP) of TriSpan, consists of its hardware and software capabilities. A description of these components and their security relevant roles are described in the following two sections.

Hardware Architecture

TriSpan's board physically consists of 64K bytes of ROM, 32K bytes of static RAM, a clock, and controlling circuitry. This circuitry, called the Controlled Access Mechanism (CAM), is used to enable TriSpan's components in the address space of the workstation. Once enabled, a separate domain for execution is established. This domain allows TriSpan to enforce access mediation, to log audited events, and to perform I&A.

The processor enters this domain when a specific sequence of instructions is executed solely on TriSpan's board. No offboard reference to memory or to an I/O port can occur or the transition will fail. If the sequence is completed fully and only within the board, TriSpan's components will be enabled on the address bus. Otherwise, the transition is aborted. This assures that control of the processor is transferred only to TriSpan's code.

Once within TriSpan domain, the processor can only reference the area enabled and still remain within the domain. All interrupts are masked out assuring control over the processor. Once TriSpan's operation is complete, an offboard reference will occur causing TriSpan's hardware to be disabled. Once disabled, TriSpan's isolated domain of execution is relinquished and the processor is transferred back to the user.

Software Architecture

This section describes the software relevant components of TriSpan's SRP including its internal programs, the MANAGER program, and commands. MANAGER and all commands reside outside of the CAM protected circuitry, but are still part of the SRP. Therefore, they must be protected. MANAGER must be protected under the administrator's GROUP identifier and commands must be protected under TriSpan's ADMIN identifier (see page 9, "Discretionary Access Control").

Internal Programs

No design documentation was supplied for this evaluation and therefore, the internal software which performs the security relevant actions for TriSpan cannot be described by the team. These programs are protected by and called through the hardware interface described on page 3, "Hardware Architecture".

MANAGER Program

The MANAGER program is used by privileged users to set the security configuration (see page 7, "Privileges"). Once the configuration has been selected, the program will pass the proper parameters to the TriSpan board so that they are installed. Specifically, MANAGER prompts for machine access requirements (e.g. password length, password expiration period, the user's PID, etc.), the auditable events, the RAC assignment, and file protection.

Although non-privileged users are not allowed to execute the MANAGER program, the file is not protected from modification when installed. Therefore, administrators must decrease this incurred risk by protecting this file with the GROUP identifier when it resides on the workstation. It should be noted that protecting MANAGER from modification on disk does not render it absolutely safe from modification while executing. The nature of DOS programs is such that the presence of foreign code, such as a Terminate and Stay Resident (TSR) program or device driver, represents a source of modification to any executing program.

For installations requiring the greatest degree of protection during modification of TriSpan's security configuration, the Central Site Administration (CSA) option should be used. This option allows the administrator to change the configuration on a physically secure workstation, bundle the new configuration file via the PACKAGE command, and deliver it to individual workstations. The ATTN command is then used to install the updated configuration on that machine. When the ATTN command is initiated, control passes through CAM before the operation can be performed within TriSpan's board (see "Command Files" below). Since the operation is performed within the board, TSRs and other programs are unable to interfere with the installation of the configuration.

It should be noted that ATTN command can be executed by any user and, since the bundled configuration file is protected under the ADMIN identifier, any user can update TriSpan's security configuration. Although the configuration file cannot be deleted or renamed by general users, only used once, and its bundling assures that bogus files cannot be used, it is preferred that an administrator perform the update operation with the ATTN command. In either case, the CSA option is preferred over executing MANAGER from a floppy disk and porting an un-bundled configuration file to each machine.

Command Files

The system is supplied with batch files used to call each command. The batch files pass the proper parameters to a program called TRIADCMD.EXE which in turn makes the proper call to TriSpan's board. The function of the command is then performed within the board and the result passed back to the system.

These commands allow all users to interact with TriSpan's capabilities and query many of its current settings. There are two types of commands, user and privileged. The user commands are used by all users to query or change that user's environment.

The privileged commands are the administrative interface to TriSpan. They allow the privileged user to maintain, monitor, and override the security configuration established by the MANAGER program.

Like the MANAGER program, the batch files and TRIADCMD.EXE are not protected when installed. Therefore, these files must be protected under the ADMIN identifier.

SRP Protected Resources

This section describes the subjects and objects that TriSpan mediates access between.

Subjects

The subjects in TriSpan are the processes performing user and system functions. A process is the abstraction of tasks which comprise a program. It consists of the current value of the program counter, registers, and associated variables. On a workstation running MS-DOS, all user processes execute in a single state. There is no separation for these processes. TriSpan's processes however, executes within a separate domain after passing through the CAM mechanism.

Objects

The objects that TriSpan protects are files, memory, and devices.

Files

Files are the basic containers in which information is stored on the IBM PC. Although files do not differ conceptually , their physical representation and location do. TriSpan protects files on floppy, hard, and RAM drives.

Memory

Memory refers to the directly addressable locations of RAM. On the workstation, this RAM is contained within the 1M addressable area of the Intel 8086, or Intel 80286 in real mode. These locations are addressable to the granularity of a single byte.

Devices

TriSpan protects ten devices. The devices consist of disk drives and communication ports. Each device is located on the I/O bus at specific port addresses. Each device is defined in the list below.

Floppy Disk Drive
Disk drives defined at port addresses 3F5H, 3F7H, 375H, and 377H.

Hard Disk
Hard drives defined at port addresses 320H to 323H.

Parallel Ports
The three parallel ports defined at addresses 278H, 27AH, 378H, 37AH, 3BCH, and 3BEH.

Asynchronous Ports
The two asynchronous ports defined at addresses 2F8H, 2F9H, 2FBH, 2FCH, 3F8H, 3F9H, 3FBH, and 3FCH.

Binary Synchronous Ports
The two binary synchronous ports defined at addresses 381H-389H except 384H, and 3A1H-3A9H except 3A4H.

Synchronous Data Link Controller (SDLC) Ports
The SDLC port defined at addresses 381H-389H and 38CH.

Network Port
The two network ports defined at addresses 360H to 36F, and 300H to 30FH.

DCA IRMA Port
The DAC port defined at addresses 220H-227H.

ARCNET port
The port addresses defined at 2E0H to 2EFH.

SRP Protection Mechanisms

This section describes TriSpan's privileges, I&A, DAC, and audit mechanisms.

Privileges

TriSpan permits only one type of privilege, the ability to implement administrative capabilities. These administrative capabilities are available to a single user, named the Workstation Administrator when TriSpan is installed. Thereafter, they can be distributed to other users if the Workstation Administrator defines assistant administrators. Assistant administrators are members of the Workstation Administrator's group (see page 8, "Group Structure").

All privileged users have the ability to execute the MANAGER program, access any protected file, and execute all of TriSpan's commands. These commands control audit capabilities, file protection, TriSpan's internal clock, and the ability to override the DAC protection on files. The ability to override DAC assures that users are unable to hold files hostage, regardless of the encryption mechanism.

Identification and Authentication

In order to access a machine on which TriSpan has been installed, a user must first pass through the I&A mechanism, a logon window. This window prompts the user for information which is described below.

An administrator must assign a Primary Identifier (PID), Secondary Identifier (SID), the allowed periods for logon, and an RAC access state (see page 11, "Resource Access Control"). The PID is the user's unique qualifier and the SID is the group name. Additionally, the administrator can require users to enter their SID, and/or a project identifier for accounting purposes, during the logon process. The administrator must then activate that user's account before the user may access the workstation.

Once this is completed, the administrator must then program an electronic token. This token contains battery backed RAM on which certain I&A information is encoded for each user. This information includes the user's PID, password, its expiration date, RAC access state, and allowed time periods of usage. The token is then issued to each user so that it can be inserted into a receptacle during logon.

Since the I&A information is contained within the token, the token can be ported to various workstations that have the same Master Phrase and have validated that user on that workstation. This provides some flexibility and distributes I&A between the user's identity, the token, and typed password. However to provide this flexibility, the authentication data (password) resides on the token and, although it is encrypted within the token and not readily accessible, the token must be safeguarded by users.

TriSpan can be configured to enforce password updates based on a minimum and maximum password lifetime defined by the administrator. When a password is updated, the user is notified during logon and after entering a new password, the token is updated. Passwords are subject to a minimum password length, and must be different than the previous password.

Each workstation running TriSpan can have a maximum of sixty-four uniquely identified users including the Workstation Administrator. As one of these sixty-four users, TriSpan supports a guest user account for which no password or token is required to logon. The guest user account is not a part of the evaluated configuration.

Group Structure

The SID is used to determine the user's group affiliation. As mentioned above, the administrator can optionally require a user to enter the SID during the logon process. However, administrators are required to assign a user to a group because it is used for file mediation. See page 9, "Discretionary Access Control" for information on the GROUP identifier. Administrators are only permitted to assigned a user to a single group so considerable forethought is necessary in determining which users will need to share files.

An important example is the assignment of the Workstation Administrator's SID to other users. Users with this SID are allowed to execute privileged commands.

The Logon Process

In order to logon, the user enters a PID. A SID and/or an account identifier may also be required if configured by an administrator. The user is then required to insert a token into the receptacle and TriSpan compares the user-supplied information with the information read from the token. Lastly, the user is prompted for a password.

If the PID, SID, password, or token data does not match the user's profile, access is denied without revealing the reason. Additionally, TriSpan can be configured such that after multiple logon failures, further attempts are suspended for a predetermined duration. An alarm can also be configured to warn those in the area. Both the lockout and alarm durations are defined by the administrator and cannot be circumvented by cycling power to the PC after they sound.

If the logon entries are correct, user access is subjected to a further test. TriSpan determines if the user is attempting to log on during a valid access period. Four different access periods can be defined by the administrator. They are specified by days of the week and hours within the day. If the user is logging on within a valid period, access to the workstation is then granted.

TriSpan also supplies a featured called suspend which is related to the I&A mechanism. This feature is automatically invoked after a fixed period of workstation inactivity or by explicit user action (i.e., the SUSPEND command is issued). Upon invocation, the workstation screen is cleared, a 'Suspend' message is displayed, and the workstation is disabled. When any key is pressed, a logon window appears and the user must go through the same procedure as an initial logon. However, only the user who is suspended can be authenticated. All other users must reset the workstation to gain access, thereby causing the suspended user to be logged off. When a suspended session is restored by the appropriate user, the interrupted application is restored to the point at which it was suspended.

Discretionary Access Control

TriSpan's DAC capability is provided through two logical mechanisms called Cryptographic Access Control (CAC) and Resource Access Control (RAC). Additionally, an option, called "Disk Manipulation Protection", must be enabled via MANAGER, to assure that disk formatting is prohibited. Generally, TriSpan's CAC mechanism monitors access to files by intercepting DOS and BIOS interrupts. The RAC mechanism prevents absolute port addressing and the disk manipulation option prevents disk formatting. The following sections describe CAC, RAC, and the option in greater detail. File access is then described in the last section.

Cryptographic Access Control

When a DOS or BIOS file operation is initiated, CAC mediates access to the file based upon the file ownership identifier encoded into the file and the current user identity. If access is allowed, CAC decrypts the file. A proprietary encryption algorithm known as SmartCypher is used to encrypt and decrypt files. This algorithm uses a key called the Master Phrase which forms the basis for TriSpan's cryptographic control. It assures that identical products do not necessarily represent the same accessible domain. This Phrase is incorporated into all protected files and tokens[1].

The evaluation team will not comment on the strength of encryption nor usage of the CAC mechanism, as these concerns are beyond the scope of a CSSI evaluation. The team found that the CAC's encryption scheme appeared to function as claimed and did not interfere with the encryption in ways other than intended.

[1] The NCSC Computer Security Subsystem Evaluation program does not evaluate encryption nor can encryption be used to meet any of the CSSI requirements. Therefore, this report cannot be considered as a comment or endorsement of the strength of TriSpan's encryption algorithm.

File protection is based upon the file ownership identifier set by the OWNER command during a logged-on session. Users are able to choose an ownership identifier or combination of identifiers so that the file has the proper level of protection or more specifically, additional identifiers lengthen the cryptographic keystream of protected files. With these identifiers, it is possible to control access based upon who can access and/or where the data is located. The file ownership identifiers are: ME, GROUP, MACHINE, COMPANY, ADMIN, and PUBLIC. It is through these identifiers that the CAC mechanism permits access and consequentially decrypts them. A description of each is given below.

ME

Files protected with the ME identifier are accessible only by the user who protected it. Access is based on the current user's PID. If it matches that of the user who protected the file, access is granted.

GROUP

Files protected with the GROUP identifier are accessible only by users who have the same SID as the user who protected it. (see page 8, "Group Structure").

MACHINE

Files protected with the MACHINE identifier are accessible only on the workstation that it was created on and then, only by users that are allowed to access the workstation (i.e. through the I&A mechanism). This is made possible though a unique phrase given to each individual workstation by the administrator. Micronyx's documentation calls this phrase the Machine Identifier (MID).

COMPANY

Files protected with the COMPANY identifier are accessible by all users that are allowed to access the workstation. COMPANY protected files are also transportable to all workstations that have the same Configuration Identifier (CID). Similar to the MID, the CID is also a phrase entered by the administrator.

ADMIN

Files protected with the ADMIN identifier can read and written by administrators. All other users can only read the file. The ADMIN identifier must be used to protect TriSpan's command files so that users are allowed to read the files, but not modify them.

PUBLIC

Files protected with the PUBLIC identifier are accessible by all users that are allowed to access the workstation. They are not encrypted.

In addition to the individual identifiers, files can be protected with multiple identifiers. Such files are accessible only by users who can pass through each identifier protecting the file. These files have a higher degree of cryptographic protection (the keystream is lengthened) and tighter control on who/where the data can be used. If an executable file, either COM or EXE, is protected by an identifier, it must be unprotected (i.e. under the PUBLIC identifier) before it can be executed and then protected again when done.

If the OWNER command is not issued with an identifier during the session, TriSpan defaults to PUBLIC. All newly created files would then be accessible by any user. Specifically, TriSpan does not provide default protection until specified by the user. To obtain a greater level of trust, a default setting of OWNER ME should appear in the AUTOEXEC.BAT file and all users should check the identifier used to protect their files after login. AUTOEXEC.BAT should then be protected under ADMIN to prevent users from modifying the batch file. Thereafter, users could still choose not to protect a file or change the settings by issuing OWNER with another identifier.

Resource Access Control

When a call is made to an I/O port address, the RAC mechanism determines if the data can be moved to or from the address. Conceptually, RAC is a limited implementation of DAC on devices because it can only permit or deny access (see page 6, "Objects"). For disk drives, this control is extended to permit either read, write, or no access to the drive. In either case, access is always based upon the permission recorded in an enumerated access state. This permission appears as "YES" or "NO" to the device in every state. For example, an administrator may allow "Hard Disk 0 READ = YES" for state 8. Administrators are allowed to define up to eight states and then define the permission allowed for each device in that state. These states are called "access levels" in Micronyx's documentation and should not be confused with the hierarchical portion of a security level as defined in the TCSEC.

Each user is then assigned one of these access states by the administrator during configuration. By default a user can only access those devices listed in his assigned state, however the administrator may configure the system so that all users have access to any devices listed in any logically lower state. This feature is referred to as Mandatory Access Control (MAC) in the TriSpan documentation. In this report, this feature will be referred to hierarchical RAC in order to avoid confusion with MAC as described in the TCSEC.

Disk Manipulation Protection

The "Disk Manipulation Protection" prevents the disk format interrupt, read logical sector, and write a logical sector interrupts. The combination of RAC and this option prevent the use of certain disk utility programs and direct access to the disk drives.

File Access & Controlling Access

The order and the specific procedure for granting access to a file is unknown because design documentation was unavailable for the evaluation. Generally, the RAC determines if authorization to the device is allowed and CAC determines if access to a file is allowed.

When a file is created, that file is assigned the access identifier(s) listed in the OWNER setting. The identifier is then encoded into the file. If multiple identifiers are active, the file will be protected by a combination of identifiers and users attempting access to the file must be permitted through each identifier before access is granted. There are two kinds of access to files: ALL or NONE. Any user with access to a file can read, write, execute (after converting it plain text), delete, and/or change the access identifiers of that file. Administrators should be aware that uncontrolled propagation of access rights can result from TriSpan's DAC. Although DOS directories are a special form of files, TriSpan does not control access to directories or sub-directories, only on the files within them.

After a file is created, the file's access identifiers can be changed by any user with access to the file. This occurs when either the PROTECT or the UNPROTECT command is executed, or when a copy is made. All users with access to a file can execute these commands. Executing the PROTECT command can change a file's access identifiers. The UNPROTECT command changes a file's access identifier to PUBLIC; converts it to plaintext. If a user copies the file, the new file takes on the access identifiers in the user's OWNER setting at the time of the copy. For example, a user can share files with other group members by saving a file after executing an OWNER GROUP command or by executing PROTECT GROUP FILENAME command after the file has been created.

Administrators should be aware of TriSpan's DAC capabilities and limitations. The CAC mechanism protects files from DOS and BIOS calls. The RAC mechanism prevents direct access to the I/O ports on which the devices reside. For a disk drive, RAC can be used to stop disk utilities and absolute control of the disk controller. However, it is impossible for the RAC mechanism to discriminate between a legitimate reference by the operating system and by an illegitimate reference by a disk editor or user written disk handler. TriSpan's RAC mechanism either allows or prevents all access. Therefore, the purpose of the disk manipulation option is intermediary. It prevents access via logical sectors, causing most disk editors to abort. Administrators can permit access to the disk drives by permitting access through RAC. However, they will be relying upon the protection of the disk manipulation option and should therefore be aware of the absolute addressing capability.

Audit

TriSpan provides the capability to create an audit trail of workstation activity. Audit must be selected from the MANAGER program before any specific event can be audited. The auditable events are:

- Logon
- Logoff
- Idle period
- Logon failure
- project identifier
- MS-DOS program execution
- MS-DOS command failure

- Session suspend
- Failure to end suspend
- I/O access violations
- File access violations
- Session summary
- Change Drive
- Change Directory
- File Open or Create
- Session
- Failure to Change Directory
- CSA Reconfigurration

The audit log for each user session contains the date and time of each event, the PID and SID, the RAC access state for the user, the machine identifier, the project code if configured, and the type of each event. The audit trail initially resides on TriSpan's static RAM. Its buffer is cyclically updated and is designed to hold 100 to 200 audit records.

As an evaluated subsystem, TriSpan must be configured to automatically write the audit records from this buffer to disk. This can be accomplished by enabling the "Audit Flush Enable" option. This option purges TriSpan audit buffer to disk when the user logs on and whenever it fills. Additionally, administrators must periodically copy the audit file to a backup medium so that the occupied disk space can be relieved.

This page intentionally left blank.

EVALUATION AS AN I&A, DAC, AND AUDIT SUBSYSTEM

This chapter of the report maps TriSpan's I&A, DAC, and audit feature requirements, to the CSSI assurance and documentation requirements. The comparisons are made against the requirements at the highest level at which the evaluation team determined TriSpan to satisfy. Where TriSpan does not satisfy a requirement, the minimum requirement is stated and the deficiency enunciated.

Identification and Authentication

Requirement

> The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

Interpretation

- D1

The I&A subsystem shall require users to identify themselves to it before beginning to perform any other actions that the system is expected to mediate. Furthermore, the I&A subsystem shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The I&A subsystem shall protect authentication data so that it cannot be accessed by any unauthorized user.

The I&A subsystem shall, at a minimum, identify and authenticate system users. At I&A/D1, users need not be individually identified.

- D2

The following interpretations, in addition to those interpretations for I&A/D1, shall be satisfied at the I&A/D2 Class.

In the TCSEC quote, "TCB" is interpreted to mean "I&A subsystem." The I&A subsystem shall pass the protected system a unique identifier for each individual.

The I&A subsystem shall be able to identify each individual user. This includes the ability to identify individual members within an authorized user group and the ability to identify specific system users such as operators, system administrators, etc.

The I&A subsystem shall provide for the audit logging of security relevant I&A events. For I&A, the origin of the request (e.g. terminal ID, etc.), the date and time of the event, user ID (to the extent recorded), type of event, and the success or failure of the event shall be recorded. The I&A subsystem may meet this requirement either through its own auditing mechanism or by providing an interface for passing the necessary data to another auditing mechanism.

Applicable Features

There are no apparent methods to bypass the login window and thus no other actions can occur before logon. In order to gain access to the workstation, users must identify and authenticate themselves. Users can be uniquely authenticated by their password taken off their token.

TriSpan possesses the capability to identify specific users based upon their PID and SID. This includes specific system users such as the workstation administrators and assistant administrators. Note, TriSpan can be configured to accept guest users, but this configuration was not evaluated as it would not meet the D2 requirement.

The authentication data resides on the token and is therefore not readily accessible. TriSpan possesses the capability to pass the identity of the user to the protected system, and its DAC and auditing components.

Conclusion

TriSpan satisfies the D2 Identification and Authentication requirement.

Discretionary Access Control

Requirement

> The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both.

Interpretation

D1:

In the TCSEC quote, "TCB" is interpreted to mean "DAC subsystem".

2.1.3.1.1 Identified users and objects

DAC subsystems must use some mechanism to determine whether users are authorized for each access attempted. At DAC/D1, this mechanism must control access by groups of users. The mechanisms that can meet this requirement include, but are not limited to:

access control lists, capabilities, descriptors, user profiles, and protection bits. The DAC mechanism uses the identification of subjects and objects to perform access control decisions. This implies that the DAC subsystem must interface with or provide some I&A mechanism. The evaluation shall show that user identities are available to DAC.

2.1.3.1.2 User-specified object sharing

The DAC subsystem must provide the capability for users to specify how other users or groups may access the objects they control. This requires that the user have a means to specify the set of authorizations (e.g., access control list) of all users or groups permitted to access an object and/or the set of all objects accessible to a user or group (e.g., capabilities).

2.1.3.1.3 Mediation

The checking of the specified authorizations of a user prior to granting access to an object is the essential function of DAC which must be provided. Mediation either allows or disallows access.

Applicable Features

TriSpan's provides discretionary access control between subjects and objects. The subjects are processes executing on the behalf of identified and authenticated users. The evaluation showed that the user identities were available to the DAC component. The identity of objects were also shown to be passed so that the access decision could be made. The objects in TriSpan are files, memory, and the TriSpan protected devices.

Files

The mechanism which allows subjects to share files are the ME, GROUP, MACHINE, COMPANY, ADMIN, and PUBLIC identifiers. These identifiers and how access mediation is performed, are described on page 9, "Discretionary Access Control". Essentially, TriSpan uses a mechanism called CAC to determine if access can be permitted based upon the identifier(s) protecting the file and the current user identity.

User's have the capability to protect a file with one or more of these identifiers. Once the identifier is specified other users have either complete or no access to a file (i.e. the set of authorizations). If access is granted, the user can alter the file or the file's access identifiers protecting it. TriSpan is not capable of controlling the propagation of access rights.

TriSpan is designed to mediate DOS and BIOS file operations to files. RAC and the "Disk Manipulation Protection" option assure that access to the disk can not be obtained, and thus to the physical sectors of the file.

Memory

TriSpan only allows a single user to be on the workstation at a time. The subjects acting for that user are able to directly manipulate all of memory residing outside of CAM control. They may therefore be able to conflict with one another, but a user is responsible for his own domain and the subjects that execute within it.

TriSpan controls access to memory by assuring that the processes of other users are not present in memory after the user logs out. This is accomplished by warm booting the workstation.

Devices

TriSpan's RAC mechanism provides access control to the three parallel ports, two asynchronous communication ports, to the synchronous data link control adapter (SDLC), the network adapter, the DCA IRMA port, the ARCNET port, and the disk drives (see page 6, "Objects").

The RAC mechanism as discussed on page 11, "Resource Access Control", can either permit or deny access to these devices based upon the configuration established by the administrator.

Although a DAC/D2 requirement, TriSpan's DAC mechanism has the capability to interface with the auditing component of itself.

Conclusion

TriSpan satisfies the D1 Discretionary Access Control feature requirement.

Audit

Requirement

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

Interpretation

The following subsections provide interpretations of the TCSEC requirements which shall be satisfied by auditing subsystems at AUD/D2.

2.4.3.1.1 Creation and management of audit trail

The auditing subsystem shall create and manage the audit trail of security-relevant events in the system. If the other portions of the system are unable to capture date about such events, the auditing subsystem shall contain the necessary interfaces into the system to perform this function. Alternatively, the auditing subsystem might simply accept and store date about events if the other portions of the system are capable of creating such data and passing them on.

2.4.3.1.2 Protection of audit data

It shall be demonstrated that the audit data is protected from unauthorized modification. This protection will be provided either by the subsystem itself or by its integration with the protected system.

2.4.3.1.3 Access control to audit

The audit mechanism, auditing parameters, and the audit data storage media shall be protected to ensure access is allowed only to authorized individuals. Individuals who are authorized to access the audit data shall be able to gain access only through the auditing subsystem.

2.4.3.1.4 Specific types of events

Data about all security relevant events must be recorded. The other portion of the system shall be able to pass data concerning these events to the auditing subsystem, or the auditing subsystem shall have the necessary code integrated into the other portions of the system to pass the data to the collection point.

2.4.3.1.5 Specific information per event

All of the specific information enumerated in the TCSEC quote shall be captured for each recorded event. Of particular concern, is the recording of the user identity with each recorded event.

2.4.3.1.6 Ability to selectively audit individuals

The auditing subsystem shall have the ability to perform selection of audit data based on individual users.

Applicable Features

TriSpan was able to create and maintain an audit log that recorded the types of events listed on page 12, "Audit". For each of these events, the log lists the PID, SID, the machine name, time, and a line of text. This text line contains either the DOS command or the action initiated. If the action failed, the type of violation is displayed.

TriSpan's DAC mechanism protects the audit log from unauthorized access. The audit log can only be read and manipulated by privileged users. Privileged users have the capability to process the audit log into readable text using the reduction tools.

Conclusion

TriSpan satisfies the D2 feature requirement for Audit.

System Architecture

Requirement

> The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

Interpretation

- D1

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform. There are two specific elements of this requirement: Execution Domain Protection and Defined Subsets.

3.1.1.1 Execution Domain Protection

Protection of the subsystem's mechanism and data from external interference or tampering must be provided. The code and data of the subsystem may be protected through physical protection (e.g., by the subsystems dedicated hardware base) or by logical isolation (e.g., using the protected system's domain mechanism).

3.1.1.2 Defined Subsets

I&A subsystems, when used for the system's I&A, define the subset of subjects under the control of the system's TCB.

DAC subsystems may protect a subset of the total collection of objects on the protected system.

Applicable Features

TriSpan's CAM mechanism maintains a protected domain for its execution. It also assures that its internal data base, internal code, and the internal buffer for the audit log cannot be modified from an external source.

TriSpan architecture protects the subset of objects as defined on page 6, "Objects". All other objects within the workstation are accessible and not protected.

Conclusion

TriSpan satisfies the D1 Subsystem Architecture requirement.

System Integrity

Requirement

> Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Interpretation

- D1

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

This requirements applies to all subsystems evaluated at any class, regardless of the functions they perform.

Applicable Features

TriSpan is supplied with a diagnostic routine to test the operation of the board. The diagnostic is only executed during installation. No indication was given if it could be executed periodically nor of its exact function.

Conclusion

TriSpan does not satisfy the D1 Integrity requirement.

Security Testing

Requirement

> The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are

> no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

Interpretation

- D1

This requirement applies to all subsystems evaluated at any class, regardless of the function(s) they perform. In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

The subsystem's Security Relevant Portion (SRP) shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected system shall not cause obvious flaws to the resulting system.

Test results shall show that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the subsystem's SRP.

- D2

This requirement applies to the testing of the SRP of any subsystem evaluated at the D2 class or the D3 class.

Applicable Features

The security mechanisms of TriSpan work as documented. When configured as per the warnings within this report and within Micronyx's documentation, there are no obvious ways for unauthorized users to bypass TriSpan's protection mechanisms. Testing also showed that there are no obvious flaws that would allow access to a protected resource or to the audit data.

Conclusion

TriSpan satisfies the D2 Security Testing requirement.

Security Features User's Guide

Requirement

> A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

Interpretation

- D1

All subsystems shall meet this requirement in that they shall describe the protection mechanisms provided by the subsystem.

- D2

There are no additional requirements at the D2 Class.

Applicable Features

A complete user manual is provided and describes TriSpan's protection mechanisms, logon procedure, commands, and other non security relevant capabilities.

Conclusion

TriSpan satisfies the D2 Security Features User's Guide requirement.

Trusted Facility Manual

Requirement

> A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

Interpretation

- D1

This requirement applies to all subsystems in that the manual shall present cautions about functions and privileges provided by the subsystem. Further, this manual shall present specific and precise direction for effectively integrating the subsystem into the overall system.

Applicable Features

The Workstation Administrator's Guide (WAG) and the WAG supplement details TriSpan's purpose, installation, access control, MANAGER, the I&A mechanism, auditing, and commands. Within these sections its privileges are presented and how they are controlled (i.e. by the Workstation Administrator's SID). The WAG and its supplement accurately reflect the product's integration into the overall system. However, the specific cautions and warnings needed to properly operate the facility are not described.

Conclusion

TriSpan does not satisfy the D1 Trusted Facility Manual requirement.

Test Documentation

Requirement

> The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.

Interpretation

- D1

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the subsystem being tested, the protected system, and other subsystems shall be described.

Applicable Features

Micronyx failed to supply any testing documentation to indicate whether the product had been exercised.

Conclusion

TriSpan does not satisfy the D1 Test Documentation requirement.

Design Documentation

Requirement

> Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Interpretation

- D1

This requirement applies directly to all subsystems. Specifically, the design document shall state what types of threats the subsystem is designed to protect against (e.g., casual browsing, determined attacks, accidents). This documentation shall show how the protection philosophy is translated into the subsystem's SRP. Design documentation shall also specify how the subsystem is to interact with the protected system and other subsystems to provide a complete computer security system. If the SRP is modularized, the interfaces between these modules shall be described.

Applicable Features

Micronyx failed to supply design documentation.

Conclusion

TriSpan does not satisfy the D1 Design Documentation requirement.

Rating Assignment

This section describes the composite feature rating and how it is determined. The composite rating for each evaluated feature is based upon the individual ratings awarded as previously described. These individual ratings are combined with ratings for assurances, documentation, and "supporting functions" (see discussion below). The resulting composite rating is equal to the lowest rating awarded in any one of the individual ratings or "supporting functions".

The CSSI requires that subsystems have "supporting functions" because the requirements rely on one another (e.g. an auditing subsystem needs the identities from the I&A subsystem). The CSSI permits a subsystem to accomplish this by alternative methods:

a. The supporting function is provided by another feature of the subsystem
b. The supporting function is provided within the feature, even though it may duplicate an aspect of another feature
c. The supporting function is provided through an interface to other products

The "supporting function" must be at the same level as that of the feature to obtain the resulting rating.

Taking the values attained in Section 3 (above), the composite ratings for each of the three features of Micronyx TriSpan are derived as shown in table 1. Note that TriSpan provides the supporting functions by integrating them within the feature. Since TriSpan does not provide all of the required assurance, documentation and supporting functions, TriSpan will be placed on the EPL as a D I&A, D DAC, and D Auditing Subsystem.

TABLE 1

EVALUATED FEATURE	INITIAL FEATURE RATING	LOWEST RATING (ASSURANCE)	LOWEST RATING (DOCUMENTATION)	REQUIRED SUPPORTING FUNCTION	SUPPORTING FUNCTION RATING	COMPOSITE FEATURE RATING
I&A	D2	D	D	AUDIT DAC*	D Yes	D
DAC	D1	D	D	I&A	D	D
AUDIT	D2	D	D	I&A DAC*	D Yes	D

* Audit and/or authentication data must be protected through DAC or domain isolation. Isolation is defined as any mechanism which prevents a subject from accessing the processes or data structures which provides the feature.

EVALUATOR'S COMMENTS

Administrators must exercise caution when programming tokens. Since they are portable among workstations with similar configurations, it is possible to configure multiple tokens or accidentally alter the data it contains. This will significantly impact on the accountability of the I&A mechanism. TriSpan displays warning screens to prevent this and they should be followed closely.

Although TriSpan can be configured without tokens. Usage of this option is not well documented and only briefly mentioned in a READ.ME file. It was unclear if all of the data normally found on the token, is duplicated on the workstation or elsewhere. Installations, especially those that install TriSpan on several workstations, should be warned that toggling between the token and tokenless option can create synchronization problems. The evaluation team has therefore, not included this option in the evaluated configuration.

TriSpan does not support the assignment of initial passwords to user accounts. As designed, TriSpan will accept any valid password during the first logon attempt and use it thereafter. This weakness can only be eliminated by administrative procedures. When an administrator creates an account, a password should be assigned and then invalidated so that it must be changed at the next successful logon.

TriSpan claims to overwrite the data contents of files at deletion. TriSpan also claims the ability to call DOS to clear memory when a user logs out. TriSpan further claims to protect files residing on LAN servers and mainframe hosts. TriSpan was not evaluated as an object reuse subsystem because it does not revoke all information from all storage objects. Although these capabilities are not part of the evaluated configuration, they may be appropriate for some installations.

This page intentionally left blank.

EVALUATED HARDWARE COMPONENTS

This appendix lists the Micronyx marketing identification numbers for all hardware covered by this evaluation. This list is equivalent to the set of hardware officially supported by this subsystem evaluation. The primary requirement for hardware is that the hardware function properly. This was verified by the diagnostic tests performed by the TriSpan board, the SYSWATCH, and the SYSCHECK programs used only during installation.

To operate in correspondence with the I&A D, DAC D, and Audit D rating, the security subsystem must contain the hardware components listed in this section.

1 TriSpan system board release 1.1230 and token receptacle. Any number of the electronic tokens used to gain access to the system.

The protected system covered by this evaluation is the IBM PC, XT, and IBM AT.

This page intentionally left blank.

EVALUATED SOFTWARE COMPONENTS

This section lists the programs that make up the various divisions of TriSpan's software. TriSpan is designed to function only on workstations using MS-DOS versions 2.1 to version 3.2.

The TriSpan Configuration Diskette Version 1.1230 contains the following files. They are associated by function below:

General Files & Programs

ARCHIVE.TRI
ALLOWBRK.EXE
ATTN.COM
PACKAGE.EXE
READ.ME
SAFECLK.EXE
TRIADCMD.EXE
TRISPAN.DFT
TRISPAN.IDX
TRISPAN.HLP

Installation Programs

INSTALLM.BAT
INSTALLU.BAT
SYSCHECK.EXE
SYSWATCH.COM

User Files & Commands

EXPORT.BAT
IMPORT.BAT
LOGOFF.BAT
OWNER.BAT
OWNERDIR.BAT
OWNERDIR.BAT
PROJECT.BAT
PROTECT.BAT
SCRIPTER.BAT
SUSPEND.BAT
SPRINT.BAT
UNPROTEC.BAT
VERSION.BAT
WHO.BAT

Administrative Files & Commands

AUDIT.BAT
AUDITACT.BAT
MANAGER.EXE
ORPHAN.BAT
OVERRIDE.BAT
PRINTAAF.BAT
PRINTC.EXE
SETCLOCK.BAT

This page intentionally left blank.

GLOSSARY

ADP	Automatic Data Processing
CAC	Cryptographic Access Control
CAM	Controlled Access Mechanism
CID	Configuration Identifier
CSSI	Computer Security Subsystem Interpretation
DAC	Discretionary Access Control
EPL	Evaluated Products List
I&A	Identification and Authentication
I/O	Input and Output
LAN	Local Area Network
MAC	Mandatory Access Control
MID	Machine Identifier
MS-DOS	Microsoft Disk Operating System
NCSC	National Computer Security Center
PID	Primary Identifier
RAC	Resource Access Control
RAM	Random Access Memory
SDLC	Synchronous Data Link Controller
SFUG	Security Features User's Guide
SID	Secondary Identifier
SRP	Security Relevant Portion
TCB	Trusted Computing Base
TCSEC	Trusted Computer Security Evaluation Criteria
TFM	Trusted Facility Manual
TSR	Terminate and Stay Resident
WAG	Workstation Administrator Guide

☆U.S. Government Printing Office : 1990 - 723-052/20264